

CLAIMS:

1. A secret file access authorization system with fingerprint limitation comprising the components as follows:

5 An authorization server provided with an authorization module, which provides a fingerprint template and an authorization secret key.

An encryption server provided with an encryption module, which generates a decryption secret key by accepting the authorization secret key provided by the authorization module, and produces the encrypted secret files by encrypting the secret
10 files to be encrypted.

A certification server provided with an authorization module, which accepts the fingerprint template provided by the authorization module, accepts the decryption secret key provided by the encryption module and the authorization secret key claiming certification that is sent by the client, and judges and confirms providing the certified
15 decryption secret key.

At least one client machine, each is provided with a user module, which embeds the kernel encryption/decryption unit into the corresponding operation system kernel of the client, accepts the authorization secret key provided by the authorization module and the decryption secret key provided by the encryption module, sends the claiming
20 certification respectively to certification module, opens the encryption/decryption unit with the certified authorization secret key and the certified decryption secret key which is returned after the certification module makes the certification,, and reads/writes the encrypted secret files.

2.A secret file access authorization system with fingerprint limitation according to
25 claim 1, the encryption server and the certification server are merged to constitute a system server, which is provided with the authorization module, the encryption module and the certification module.

3. A secret file access authorization system with fingerprint limitation according to claim 1, the authorization server and the encryption server are merged to constitute an
30 authorization-and-encryption server, which is provided with the authorization module and the encryption module.

4. A secret file access authorization system with fingerprint limitation according to

claim 1, the authorization server and the certification server are merged to constitute an authorization-and-certification server, which is provided with the authorization module and the certification module.

5 5. A secret file access authorization system with fingerprint limitation according to claim 1, the encryption server and the certification server are merged to constitute an encryption-and-certification server, which is provided with the encryption module and the certification module.

10 6. A secret file access authorization system with fingerprint limitation according to claim 1-5, the authorization module includes a password fingerprint unit, an environment fingerprint sampling unit and a time fingerprint sampling unit, which are set in parallel, as well as the authorization unit that is linked with the said three units which are set in parallel respectively by the bidirectional programs; the authorization unit provides the authorization secret key; while the password fingerprint unit, the environment fingerprint sampling unit and the time fingerprint sampling unit that are
15 set in parallel provide the fingerprint template altogether.

7. A secret file access authorization system with fingerprint limitation according to claim 6, the authorization secret key is a binary string of a certain length.

8. A secret file access authorization system with fingerprint limitation according to claim 7, the authorization secret key can be put into the authorized entity.

20 9. A secret file access authorization system with fingerprint limitation according to claim 6, the fingerprint template is a binary string of a certain length.

10. A secret file access authorization system with fingerprint limitation according to claim 1-5, the encryption module includes the secret key generation unit and the encryption unit, which are linked in sequence by the programs; the secret key
25 generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

30 11. A secret file access authorization system with fingerprint limitation according to claim 10, the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

12. A secret file access authorization system with fingerprint limitation according

to claim 10, the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

13. A secret file access authorization system with fingerprint limitation according to claim 1-5, the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; the certification interface unit linked with them by the bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

14. A secret file access authorization system with fingerprint limitation according to claim 1-5, the user module includes the application unit, the kernel encryption/decryption unit and the input/output unit, which are linked in sequence by the bidirectional programs; as well as the authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; and the input/output unit is coupled with the encrypted secret files bidirectionally; the kernel encryption/decryption unit is embedded in the client operation system kernel.

15. A secret file access authorization system with fingerprint limitation according to claim 14, the client operation system can be Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

16. A secret file access authorization system with fingerprint limitation according to claim 14, the program used by the application unit can be Microsoft Office and its components or other desktop applications or embedded applications.